

### **REMARKS**

The following remarks are prepared in response to the Office Action mailed May 4, 2005. Claims 1-3, 5-20, 22-36, 38-51 and 53-56 are pending in this application, after entry of this amendment.

Claims 1-56 were rejected under 35 U.S.C. §102(e) as being anticipated by *Reid et al.* (U.S. Patent No. 6,182,226, hereinafter *Reid*). Applicant respectfully traverses and requests reexamination.

#### **Rejection Under 35 U.S.C. §102(e)**

##### **Independent Claim 1**

The rejection of claim 1 should be withdrawn as *Reid* fails to disclose all the recitations of amended claim 1 and therefore does not anticipate this claim. Claim 1 has been amended to include the features of claim 4.

Focusing on the specific recitations of amended claim 1 and the inadequacies of *Reid*, amended claim 1 recites, among other things: A secure network having a plurality of anti-bubbles, each anti-bubble having a plurality of anti-bubble partitions, each anti-bubble partition having no network connectivity to all other anti-bubble partitions within the same anti-bubble.

The term “anti-bubble” is intended to refer to two or more devices that have no network access or connectivity with each other. (See paragraph 27 of the patent application.) Members of an anti-bubble have no network connectivity to any other members of the same anti-bubble. (See paragraph 49 of the patent application.) Moreover, members of any anti-bubble partition have no network connectivity to members of any other anti-bubble partition within the same anti-bubble. (See paragraph 49 of the patent application.) For example, as shown in figure 2, a device in anti-bubble partition 20a does not have network connectivity to any device in anti-bubble partition 20a or anti-bubble partition 20b.

On page 4 of the Office Action, the Examiner incorrectly states that *Reid* discloses the claimed limitation in col. 3, lns. 66-67 and col. 4, lns. 1-10 wherein each of the plurality of antibubble partitions has no network connectivity to all other antibubble partitions within the same antibubble. The Examiner is incorrectly analogizing an antibubble partition as recited in claim 1 with an application-level gateway as disclosed in *Reid*. An anti-bubble partition separates two bubble devices of the same bubble and does not allow a network connection between the two bubble devices. By contrast, an application-level gateway (e.g., secure zone 34 in FIG. 1) negotiates communications and never makes a direct connection between two different networks. (See col. 3, ln. 66 to col. 4, ln. 1.) In *Reid*, since the application-level gateway negotiates communications, there must be a connection between the two different networks, but not a direct connection. That is, the connection of the two different networks is made through the application-level gateway.

By contrast, claim 1 recites each anti-bubble partition having no network connectivity to all other anti-bubble partitions within the same anti-bubble. *Reid* fails to disclose a network where a region of the network has no network access or connectivity with another region of the network. Rather, *Reid* allows indirect connections between two different networks. Therefore, for at least the reasons discussed above, *Reid* does not disclose, teach or suggest all the features of claim 1. Accordingly, the rejection of claim 1 under 35 U.S.C. §102(e) should be withdrawn.

#### **Independent Claim 17**

The rejection of claim 17 should be withdrawn as *Reid* fails to disclose all the recitations of amended claim 17 and therefore does not anticipate this claim. Claim 17 has been amended to include the features of claim 21.

Focusing on the specific recitations of amended claim 17 and the inadequacies of *Reid*, amended claim 17 recites, among other things: A secure network having a plurality of

network control points, each network control point enforces source integrity for all of the plurality of anti-bubble partitions that are connected to it.

On page 5 of the Office Action, the Examiner incorrectly states that *Reid* discloses the claimed limitation in col. 6, lns. 47-56 and col. 8, lns. 43-57 wherein the plurality of network control points ensure source address integrity across the virtual backbone. The Examiner is incorrectly analogizing source integrity as recited in claim 17 with source address rewrites as disclosed in *Reid*. Source integrity is commonly referred to as anti-spoofing and means that a router will block data marked as originating from an address that is not part of the valid address range for a particular interface. (Para. 57 of the present application.) By way of example, for lower level networks, a media access control (MAC) address can be checked for validity against a list of known addresses. (Para. 57 of the present application.) Ensuring source integrity does not entail an IP address rewrite as disclosed in *Reid*. (See col. 6, ln. 45 to col. 6, ln. 56.) In *Reid*, a rewrite node is a point in an access rule where source or destination addresses are mapped to other source or destination addresses. Destination IP address rewrites allow an inbound connection through network address translation (NAT) address hiding to be remapped to a destination inside the NAT barrier.

By contrast, claim 17 recites each network control point enforces source integrity for all of the plurality of anti-bubble partitions that are connected to it. *Reid* fails to disclose a network where source address is achieved by checking for validity against a list of known addresses. Therefore, for at least the reasons discussed above, *Reid* does not disclose, teach or suggest all the features of claim 17. Accordingly, the rejection of claim 17 under 35 U.S.C. §102(e) should be withdrawn.

### **Independent Claim 34**

The rejection of claim 34 should be withdrawn as *Reid* fails to disclose all the recitations of amended claim 34 and therefore does not anticipate this claim. Claim 34 has been amended to include the features of claim 37.

Focusing on the specific recitations of amended claim 34 and the inadequacies of *Reid*, amended claim 34 recites, among other things: A secure network having a plurality of anti-bubbles, each anti-bubble having a plurality of anti-bubble partitions, wherein no data can be transmitted between two devices in different anti-bubble partitions of the same anti-bubble.

On page 5 of the Office Action, the Examiner incorrectly states that *Reid* discloses the claimed limitation in col. 16, lns. 50-67 wherein data is not transmitted between two network devices in different antibubble partitions of the same antibubble. Claim 34 recites the opposite of *Reid*. In *Reid*, the data packet is forwarded to the real destination if the destination is in the same region as the source and the router flag is set for that region. (See col. 16, ln. 50-57.) By contrast, claim 34 recites that no data can be transmitted between two devices in different anti-bubble partitions of the same anti-bubble. Therefore, *Reid* actually teaches away from the present invention as recited in claim 34. *Reid* fails to disclose a network where no data can be transmitted between two devices in different anti-bubble partitions of the same anti-bubble. Therefore, for at least the reasons discussed above, *Reid* does not disclose, teach or suggest all the features of claim 34. Accordingly, the rejection of claim 34 under 35 U.S.C. §102(e) should be withdrawn.

### **Independent Claim 48**

The rejection of claim 48 should be withdrawn as *Reid* fails to disclose all the recitations of amended claim 48 and therefore does not anticipate this claim. Claim 48 has been amended to include the features of claim 52.

Focusing on the specific recitations of amended claim 48 and the inadequacies of *Reid*, amended claim 48 recites, among other things: A secure network having a plurality of anti-bubbles, a plurality of bubbles, and a plurality of network control points, wherein the plurality of network control points are coupled to one another and form a virtual backbone that is external to all of the plurality of anti-bubbles and bubbles.

On page 5 of the Office Action, the Examiner incorrectly states that *Reid* discloses the claimed limitation in col. 8, lns. 43-57 wherein the plurality of network control points are coupled to one another and form a virtual backbone that is external of all of the plurality of antibubbles. The Examiner is incorrectly analogizing a virtual backbone as recited in claim 48 with a virtual private network (VPN) as disclosed in *Reid*. The term “virtual backbone” refers to a network that connects a plurality of network control points having the property of source integrity (e.g., anti-spoofing). (Para. 36 of the present application.) The virtual backbone is external to all of the anti-bubbles and network control points. (Para. 36 of the present application.) Regarding the virtual backbone, the source address of all anti-bubble partitions and bubble partitions must be strictly enforced at the network control points and integrity of the source address must be maintained in all virtual backbone links, which interconnect network control points. (Para. 64 of the present application.) The minimum network security policy for the virtual backbone is that it will enforce source address integrity on its external connections, that is, not allowing external networks to send data that masquerade as being sourced from address space included in a known bubble or anti-bubble implemented, or reserved for implementation. (Para. 64 of the present application.)

By contrast, a virtual private network (VPN) is a method of authenticating and transparently encrypting bi-directional data transmissions via the Internet. (See col. 8, lns. 50-52.) In *Reid*, the VPN provides authentication and encryption but does not enforce source address integrity on its external connections. Claim 48 recites a virtual backbone, which is a

network that connects a plurality of network control points having the property of source integrity (e.g., anti-spoofing). *Reid* fails to disclose a plurality of network control points that are coupled to one another and form a virtual backbone that is external to all of the plurality of anti-bubbles and bubbles. Therefore, for at least the reasons discussed above, *Reid* does not disclose, teach or suggest all the features of claim 48. Accordingly, the rejection of claim 48 under 35 U.S.C. §102(e) should be withdrawn.

**Dependent Claims 2, 3, 5-16, 18-20, 22-33, 35, 36, 38-47, 49-51 and 53-56**


Claims 2, 3 and 5-16 depend from independent claim 1, claims 18-20 and 22-33 depend from independent claim 17, claims 35, 36 and 38-47 depend from independent claim 34, and claims 49-51 and 53-56 depend from independent claim 48. All of these dependent claims define the secure network with greater particularity and thus further distinguish over *Reid*. For these reasons, and for the reasons set forth above with respect to independent claims 1, 17, 34 and 48, the rejection of these dependent claims should be withdrawn.

**Conclusion**

If there are any questions with regards to this prosecution, or if the Examiner believes that a telephone interview will help further the prosecution of the case, she is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on August 4, 2005.

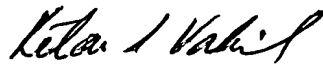
By: Lori Lapidario

  
\_\_\_\_\_  
Signature

Dated: August 4, 2005

Very truly yours,

**SNELL & WILMER L.L.P.**

  
\_\_\_\_\_  
Ketan S. Vakil  
Registration No. 43,215  
600 Anton Boulevard, Suite 1400  
Costa Mesa, California 92626-7689  
Telephone: (714) 427-7405